Remarks

Reconsideration of the above-captioned application is respectfully requested. Claim 1 has been rejected under 35 U.S.C. §102 as being anticipated by Yokota et al., USPN 6,691,149 and as being anticipated by Knauft, USPP 2001/0029581. Also, Claims 1, 23-26, and 41-46 has been rejected as being anticipated by Richards, USPN 6,690,795. Claims 2-16 and 47 have been rejected under 35 U.S.C. §103 as being unpatentable over any one of the above references in view of Ishiguro et al., USPP 2002/0083319, and Claims 27-40 and 48 have been rejected as being unpatentable over Richards in view of Ishiguro et al. A provisional double patenting rejection has been levied against Claims 1-22 based on USPA SN 09/770,877 in view of all four of the above references plus the Schneier article. However, since the co-pending application is the parent application of this one, this application has the same priority date as the co-pending application as to everything relied on in the co-pending application. Moreover, since the rejection is provisional only, the issue is insufficiently ripe to warrant paying more fees in the form of a Terminal Disclaimer until such time as this application is otherwise allowable and the parent application actually issues.

To overcome the rejections, Claim 2 limitations have been moved into Claim 1, and Claim 26 and 27 limitations have been moved into Claim 24.

Rejections Under 35 U.S.C. §102

The examiner is reminded that rejections should be strictly confined to the best available art. Cumulative rejections should be avoided, MPEP §706.02.

Claim 1 has been rejected under 35 U.S.C. §102 as being anticipated by Yokota et al., USPN 6,691,149 and as being anticipated by Knauft, USPP 2001/0029581. Both of these rejections are now moot.

Also, Claims 1, 23-26, and 41-46 have been rejected as being anticipated by Richards, USPN 6,690,795. The rejections of Claims 41-46 remain at issue.

Turning first to independent Claim 41 and using the below table to juxtapose the claimed elements with the relied-upon keys from Figure 17 of Richards, it can be seen that Richards has been misread.

Claim 41	**Richards**
session key K_s obtained with device key K_d;	segment key obtained with customer code;
channel unique key K_{cu} obtained with K_s;	channel access key obtained using segment key;
title key K_t obtained using K_{cu};	program key obtained using channel access key;
K_T decrypts content.	"program key" decrypts content.

In the above table, the terms used by the examiner in the rejection are set forth under "Richards". Setting aside for the moment the evident eradication of certain claim terms presumably under the guise of broad claim interpretation during prosecution, in Richards it is untrue that his segment key (Sk) is decrypted with a customer code as otherwise alleged. Instead, his channel control key CCk is what is decrypted using the customer's channel access key CAk. It is equally untrue that Richards' channel access key CAk is decrypted with the segment key. Instead, the segment key is used to decrypt content, and is itself decrypted by the program key Pk, not the channel access key. Moreover, the allegation is incorrect that the program key of Richards is decrypted using the channel access key. Instead, it is decrypted using the channel control key CCk. Moreover, the program key of Richards, contrary to the rejection, does not decrypt content. It decrypts the segment key Sk, which is what is used to decrypt content.

In the event that the examiner is engaged in renaming keys of Richards to fit the rejection, he must (1) explain where Richards gives him license to do this, and (2) explain why the first of the claimed decrypted keys (the session key Ks) should be regarded to be the first of the decrypted keys of Richards (in reality, the channel control key CCk), why the second of the claimed decrypted keys (the channel unique key) should be regarded not as the channel control key but instead as the program key of Richards, and why the third of the claimed decrypted keys (the title key, which decrypts content) should be regarded not as the segment key of Richards, which decrypts content, but instead as the program key, which does not decrypt content but which decrypts the segment key Sk. And so the circle is completed - in undertaking these explanations, the examiner should explain why the skilled artisan would regard, e.g., the second decrypted key of Claim 41 (modified as being "channel unique") is read upon by the second decrypted key of Richards (the program key), which is nowhere said by Richards to be unique to any channel, and so on, see MPEP §2111.01 (claims may be interpreted only so broadly as the skilled artisan would interpret them).

Turning now to independent Claim 44, the same convenient juxtaposition of the claim elements with the relied-upon elements of Richards shall be used:

Claim 44	**Richards**
receiving private information I_u upon reg.	header of packet "2" in fig. 1
subscribing to at least one channel	background discussion col. 3, lines 7-12
receiving an encrypted channel key K_c in response to subscribing	CCk, fig. 14
deriving the channel key K_c using I_u; and	unexplained

using K_c to decrypt streamed content CCk, figure 14.

The defects in the rejection can be seen as follows. First, nowhere does Richards discuss that the relied-upon header of packet "2" is received upon registration. The packet is sent with a TV program independently of registration. Second, there is no citation to any teaching that "private" information of any kind is in the header. More importantly, there is no citation to anything that indicates the packet header is used to "derive" anything, much less the relied-upon CCk, probably why this allegation is made without further explication by simply repeating the claim.

Rejections Under 35 U.S.C. §103

Claims 2-16 and 47 have been rejected under 35 U.S.C. §103 as being unpatentable over any one of the above references in view of Ishiguro et al., USPP 2002/0083319, and Claims 27-40 and 48 have been rejected as being unpatentable over Richards in view of Ishiguro et al.

Of relevance to amended Claims 1 and 24 is the rejection of Claim 2, alleging that Ishigaro et al. obtains a channel unique key (relying on "e") by combining a channel key (relying on "e1") with a session key (relying on "e2"). Once again, the examiner is ignoring claim terms that have meaning. The relied-upon keys e1 and e2 are encrypted versions of session keys. Neither is said to be in any way uniquely related to a channel, nor has the examiner explained this discrepancy. The session keys appear to be generated in the DVD and thus function more like device keys, but in any event, Ishiguro et al. does not even mention the word "channel" anywhere in its text. The examiner is either making things up out of non-existent teachings of Ishiguro et al., or is writing the modifier "channel unique" out of the claim.

Equally problematic is the superficiality with which the *prima facie* case has been made. Recall that Ishiguro et al. has been proposed to be combined "with any" of the three primary references, but no reference-specific analysis of why it would be obvious to combine the secondary reference with each of the very different, individual primary references has been offered. Instead, the sole reason proferred for the proposed combination is that Ishiguro et al. "teaches that the channel-unique key can be obtained only by a player that is compliant with both copy protection rules and subscription rules", relying on "Abstract and figure 4".

First, the proferred suggestion to combine is flat-out wrong. Nowhere do either the abstract or figure 4 mention what the examiner alleges they do. Indeed, the text of the reference nowhere contains the words "subscription" or "subscribe."

Next, what must be explained is how and why a relied-upon suggestion in a secondary reference relates to a primary reference. There must be something, in other words, tying the relied-upon suggestion specifically to a primary reference. Otherwise, since almost every patent extols its virtues in a vacuum, the fundamental *sine qua non* of patentability - the requisite prior art suggestion to combine - would be eviscerated. In the present case, this would require, for each primary reference sought to be modified by the secondary reference,

(1) identifying a suggestion to modify the cited reference(s) as proposed by the Examiner to arrive at the instant claimed invention;

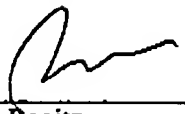
(2) setting forth why the Examiner believes that a reasonable expectation of success exists for the proposed modification of the references which would be necessary to arrive at the claimed subject matter; and

(3) explaining where in the prior art all of the claimed limitations are taught or suggested, MPEP §2143.

The fact that Applicant has focussed its comments distinguishing the present claims from the applied references and countering certain rejections must not be construed as acquiescence in other portions of rejections not specifically addressed. By way of non-limiting example, it does not appear that the device keys of Ishiguro et al. are used to activate the player, as otherwise recited in Claim 5, nor does anything resembling a key block, much less a session key block, appear in the secondary reference as otherwise recited in Claim 9, much less still the further delimiting steps of Claims 10-17.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1033-130.AMD